1 Migrating from CycloneCrypto 1.8.6 to 1.9.0

No changes required. Version 1.9.0 can be used as drop-in replacement.

2 Migrating from CycloneCrypto 1.8.2 to 1.8.6

No changes required. Version 1.8.6 can be used as drop-in replacement.

3 Migrating from CycloneCrypto 1.8.0 to 1.8.2

No changes required. Version 1.8.2 can be used as drop-in replacement.

4 Migrating from CycloneCrypto 1.7.8 to 1.8.0

The “cyclone_crypto” folder has been reorganized. Cryptographic algorithms are now sorted by family (hash, cipher, MAC, etc). Your project or makefile must be modified in order to reflect the new file structure:

Old filenames (version 1.7.8)	New filenames (version 1.8.0)
cyclone_crypto/crypto.h	cyclone_crypto/core/crypto.h
cyclone_crypto/md5.c cyclone_crypto/md5.h	cyclone_crypto/hash/md5.c cyclone_crypto/hash/md5.h
cyclone_crypto/sha1.c cyclone_crypto/sha1.h	cyclone_crypto/hash/sha1.c cyclone_crypto/hash/sha1.h
cyclone_crypto/sha224.c cyclone_crypto/sha224.h	cyclone_crypto/hash/sha224.c cyclone_crypto/hash/sha224.h
cyclone_crypto/sha256.c cyclone_crypto/sha256.h	cyclone_crypto/hash/sha256.c cyclone_crypto/hash/sha256.h
cyclone_crypto/sha384.c cyclone_crypto/sha384.h	cyclone_crypto/hash/sha384.c cyclone_crypto/hash/sha384.h
cyclone_crypto/sha512.c cyclone_crypto/sha512.h	cyclone_crypto/hash/sha512.c cyclone_crypto/hash/sha512.h
cyclone_crypto/hmac.c cyclone_crypto/hmac.h	cyclone_crypto/mac/hmac.c cyclone_crypto/mac/hmac.h
cyclone_crypto/poly1305.c cyclone_crypto/poly1305.h	cyclone_crypto/mac/poly1305.c cyclone_crypto/mac/poly1305.h
cyclone_crypto/rc4.c cyclone_crypto/rc4.h	cyclone_crypto/cipher/rc4.c cyclone_crypto/cipher/rc4.h
cyclone_crypto/idea.c cyclone_crypto/idea.h	cyclone_crypto/cipher/idea.c cyclone_crypto/cipher/idea.h
cyclone_crypto/des.c cyclone_crypto/des.h	cyclone_crypto/cipher/des.c cyclone_crypto/cipher/des.h
cyclone_crypto/des3.c cyclone_crypto/des3.h	cyclone_crypto/cipher/des3.c cyclone_crypto/cipher/des3.h
cyclone_crypto/aes.c cyclone_crypto/aes.h	cyclone_crypto/cipher/aes.c cyclone_crypto/cipher/aes.h
cyclone_crypto/camellia.c cyclone_crypto/camellia.h	cyclone_crypto/cipher/camellia.c cyclone_crypto/cipher/camellia.h
cyclone_crypto/aria.c cyclone_crypto/aria.h	cyclone_crypto/cipher/aria.c cyclone_crypto/cipher/aria.h
cyclone_crypto/seed.c cyclone_crypto/seed.h	cyclone_crypto/cipher/seed.c cyclone_crypto/cipher/seed.h
cyclone_crypto/chacha.c cyclone_crypto/chacha.h	cyclone_crypto/cipher/chacha.c cyclone_crypto/cipher/chacha.h
cyclone_crypto/cipher_mode_cbc.c cyclone_crypto/cipher_mode_cbc.h	cyclone_crypto/cipher_mode/cbc.c cyclone_crypto/cipher_mode/cbc.h
cyclone_crypto/cipher_mode_ccm.c cyclone_crypto/cipher_mode_ccm.h	cyclone_crypto/aead/ccm.c cyclone_crypto/aead/ccm.h
cyclone_crypto/cipher_mode_gcm.c cyclone_crypto/cipher_mode_gcm.h	cyclone_crypto/aead/gcm.c cyclone_crypto/aead/gcm.h
cyclone_crypto/chacha20_poly1305.c cyclone_crypto/chacha20_poly1305.h	cyclone_crypto/aead/chacha20_poly1305.c cyclone_crypto/aead/chacha20_poly1305.h
cyclone_crypto/dh.c cyclone_crypto/dh.h	cyclone_crypto/pkc/dh.c cyclone_crypto/pkc/dh.h

cyclone_crypto/rsa.c cyclone_crypto/rsa.h	cyclone_crypto/pkc/rsa.c cyclone_crypto/pkc/rsa.h
cyclone_crypto/dsa.c cyclone_crypto/dsa.h	cyclone_crypto/pkc/dsa.c cyclone_crypto/pkc/dsa.h
cyclone_crypto/mpi.c cyclone_crypto/mpi.h	cyclone_crypto/mpi/mpi.c cyclone_crypto/mpi/mpi.h
cyclone_crypto/base64.c cyclone_crypto/base64.h	cyclone_crypto/encoding/base64.c cyclone_crypto/encoding/base64.h
cyclone_crypto/asn1.c cyclone_crypto/asn1.h	cyclone_crypto/encoding/asn1.c cyclone_crypto/encoding/asn1.h
cyclone_crypto/oid.c cyclone_crypto/oid.h	cyclone_crypto/encoding/oid.c cyclone_crypto/encoding/oid.h
cyclone_crypto/pem.c cyclone_crypto/pem.h	cyclone_crypto/certificate/pem_import.c cyclone_crypto/certificate/pem_import.h
cyclone_crypto/x509.c cyclone_crypto/x509.h	cyclone_crypto/certificate/x509_common.c cyclone_crypto/certificate/x509_common.h cyclone_crypto/certificate/x509_cert_import.c cyclone_crypto/certificate/x509_cert_import.h cyclone_crypto/certificate/x509_cert_validate.c cyclone_crypto/certificate/x509_cert_validate.h
cyclone_crypto/yarrow.c cyclone_crypto/yarrow.h	cyclone_crypto/rng/yarrow.c cyclone_crypto/rng/yarrow.h

Remark: The x509.c source file has been replaced by a set of 3 distinct files (x509_common.c, x509_cert_parse.c and x509_cert_validate.c)

A new naming convention is used for ASM files (mpi_architecture_compiler.extension). If assembler optimization is used in your project to accelerate MPI calculation, then your makefile must be modified as follows:

Old filenames (version 1.7.8)	New filenames (version 1.8.0)
cyclone_crypto/mpi_asm_keil_arm7.s	cyclone_crypto/mpi/mpi_arm_v4_keil.s
cyclone_crypto/mpi_asm_keil_cortex_m3.s	cyclone_crypto/mpi/mpi_arm_v7m_keil.s
cyclone_crypto/mpi_asm_iar_cortex_m3.s	cyclone_crypto/mpi/mpi_arm_v7m_iar.s
cyclone_crypto/mpi_asm_gcc_cortex_m3.S	cyclone_crypto/mpi/mpi_arm_v7m_gcc.S
cyclone_crypto/mpi_asm_gcc_cortex_a9.S	cyclone_crypto/mpi/mpi_arm_v7a_gcc.S
cyclone_crypto/mpi_asm_gcc_cortex_mips.S	cyclone_crypto/mpi/mpi_mips_gcc.S